

AMENDMENTS TO THE CLAIMS

1 1. (Currently Amended) An architecture for confirming the identity of a
2 message sender on a remote services system, comprising:
3 a communications module operable to transmit a message;
4 a cryptographic module in said communication module for providing encryption
5 of a data stream in said message, said cryptographic module comprising
6 secure sockets layer encryption;
7 a mid-level manager operating in said remote services system in conjunction with
8 said communications module for controlling the flow of messages in said
9 remote services system between a customer proxy and an applications
10 server and for verifying the identity of a sender by comparing first and
11 second data identities in said data stream, wherein said first data identity
12 comprises data in a network software layer, said second data identity
13 comprises data in an application software layer.

1 2. (Canceled)

1 3. (Canceled)

1 4. (Canceled)

1 5. (Currently Amended) The architecture according to claim 4 1, wherein
2 said mid-level manager is a customer mid-level manager.

1 6. (Currently Amended) The architecture according to claim 4 1, wherein
2 said mid-level manager is an aggregation mid-level manager.

1 7. (Currently Amended) The architecture according to claim 2 1, wherein
2 transmission of said message is conditioned on HTTP.

1 8. (Currently Amended) The architecture according to claim 2 1, wherein
2 transmission of said message is conditioned on email protocol.

1 9. (Previously Presented) A method of confirming the identity of a
2 message sender on a remote services system, comprising:
3 obtaining a first identity related to a message, said first identity being obtained
4 from a network software layer in said remote services system;
5 obtaining a second identity related to the sender of a messages, said second
6 identity being obtained from an application software layer in said remote
7 services system; and
8 comparing said first identity with said second identity to verify the identity of the
9 sender of said message.

1 10. (Canceled)

1 11. (Original) The method according to claim 10, further comprising
2 encrypting said message and said identities in an encryption module in said remote
3 services system.

1 12. (Original) The method according to claim 11, said encryption of said
2 data and said identities being performed in accordance with secure socket layer protocol.

1 13. (Original) The method according to claim 12, said message being
2 transmitted in said system using HTTP protocol.

1 14. (Original) The method according to claim 12, said message being
2 transmitted in said system using email protocol.

1 15. (Currently Amended) A method of confirming the identity of a message
2 sender on a remote services system, comprising:
3 transmitting a message using a communications module of said remote services
4 system;
5 encrypting a data stream in said message using an encryption module in said
6 communications module, said encryption module comprising secure
7 sockets layer encryption; and

8 controlling the flow of said message between a customer proxy and an
9 applications server in said remote services system using a mid-level
10 manager, said mid-level manager verifying the identity of a sender by
11 comparing first and second data identities in said data stream, wherein said
12 first identity comprises encrypted data in a network software layer of said
13 remote services system, said second identity comprises encrypted data in
14 an application software layer of said remote services system.

1 16. (Canceled)

1 17. (Canceled)

1 18. (Canceled)

1 19. (Original) The method according to claim 15, wherein said mid-level
2 manager is a customer mid-level manager.

1 20. (Original) The method according to claim 15, wherein said mid-level
2 manager is an aggregation mid-level manager.